

PTAB Oral Argument

May 6, 2024

KEYSIGHT TECHNOLOGIES, INC.

and PALO ALTO NETWORKS, INC. v. CENTRIPETAL NETWORKS, LLC

PETITIONERS

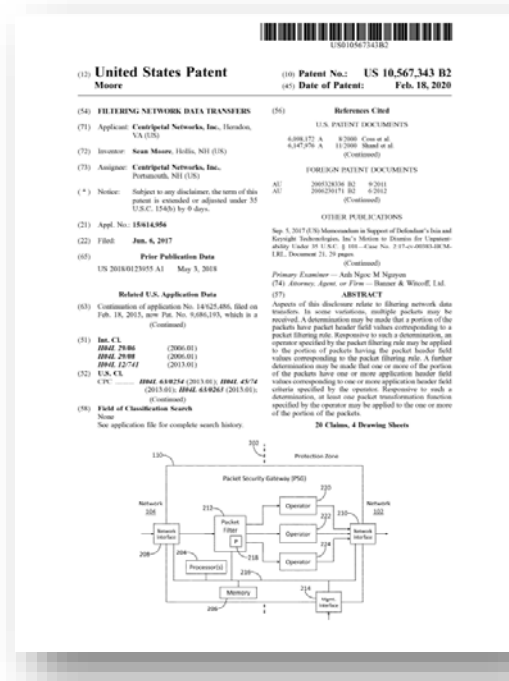
PATENT OWNER

CASE: IPR2023-00446 (U.S. PAT NO. 10,567,343)

JOINED WITH: IPR2023-01353

'343 Patent: Preventing Exfiltrations

- Cyber-attacks known as **exfiltrations** “had proven to be especially difficult for conventional cyber defense systems to prevent”
 - Others’ prior attempts: “too coarse”, “overbroad”, “resulting in negative impact to” networks
- The inventors recognized and solved the problem of preventing exfiltrations “while still preserving the flow of normal legitimate network traffic without disruption.”



POR at 10-13; '343 Pat at 1:28-31, 7:35-40; Ex. 1085 at 112, ¶ 11

'343 Patent – Claim 1

1. A method comprising:

- receiving, by a computing system comprising memory and at least one processor, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;
- determining, based on a packet header field value, whether each packet of the plurality of packets comprises data corresponding to first criterion specified by one or more packet-filtering rules;
- responsive to a determination by the computing system that a packet header field value of the first portion of packets comprises data corresponding to the first criterion specified by at least one matching packet-filtering rule, applying, by the computing system and to each packet in the first portion of packets, one or more operators specified by the at least one matching packet-filtering rule;
- determining, based on an application header field value, the second portion of packets based on whether the first portion of packets comprises data corresponding to second criterion specified by one or more operators specified by the at least one matching packet-filtering rule; and
- responsive to determining the second portion of packets that comprises data corresponding to the second criterion specified by one or more operators specified by the at least one matching packet-filtering rule, applying, by the computing system and to each packet in the second portion of packets that match the second criterion, at least one packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.

'343 Patent – Claim 8

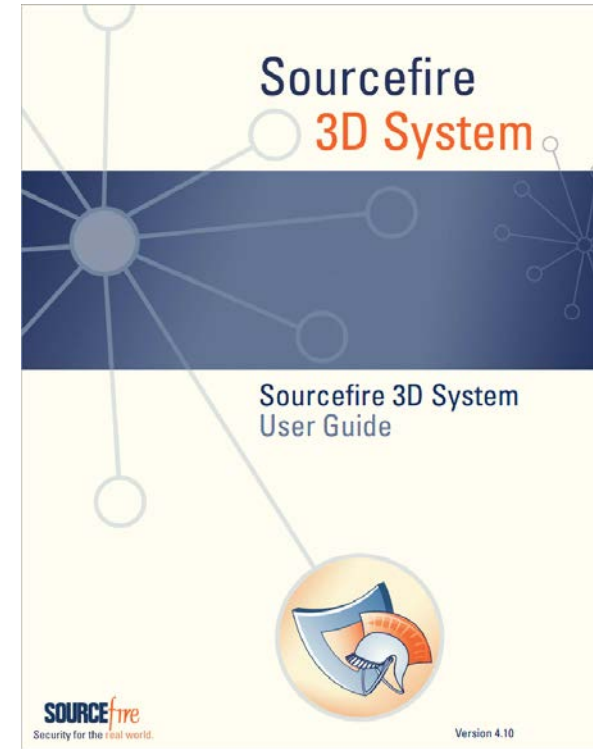
- 8. An apparatus comprising:
 - at least one processor; and
 - memory storing instructions that, when executed by the at least one processor, cause the apparatus to:
 - receive a plurality of packets;
 - determine, based on a packet header field value, whether the plurality of packets comprises data corresponding to first criterion specified by one or more packet-filtering rules;
 - responsive to a determination that a packet header field value of a first portion of packets comprises data corresponding to the first criterion specified by at least one matching packet-filtering rule, apply, to each packet in the first portion of packets, one or more operators specified by the at least one matching packet-filtering rule;
 - determine, based on an application header field value, a second portion of packets based on whether the first portion of packets comprises data corresponding to second criterion specified by one or more operators specified by the at least one matching packet-filtering rule; and
 - responsive to determining the second portion of packets that comprises data corresponding to the second criterion specified by one or more operators specified by the at least one matching packet-filtering rule, apply, to each packet in the second portion of packets, at least one packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.

'343 Patent – Claim 15

- 15. One or more non-transitory computer-readable media comprising instructions that, when executed by one or more computing devices, cause the one or more computing devices to:
 - receive a plurality of packets;
 - determine, based on a packet header field value, whether the plurality of packets comprises data corresponding to first criterion specified by one or more packet-filtering rules;
 - responsive to a determination that a packet header field value of a first portion of packets comprises data corresponding to the first criterion specified by at least one matching packet-filtering rule, apply, to each packet in the first portion of packets, one or more operators specified by the at least one matching packet-filtering rule;
 - determine, based on an application header field value, a second portion of packets based on whether the first portion of packets comprises data corresponding to second criterion specified by one or more operators specified by the at least one matching packet-filtering rule; and
 - responsive to determining the second portion of packets that comprises data corresponding to the second criterion specified by one or more operators specified by the at least one matching packet-filtering rule, apply, to each packet in the second portion of packets that match the second criterion, at least one packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.

Sourcefire (Ex. 1004)

- 2,123-page manual for Sourcefire 3D System
- Includes syntax guide on Snort rules (“Chapter 20: Understanding and Writing Intrusion Rules”) (p761-877)
- No mention of **exfiltration** whatsoever



Prior Proceedings

- The Office has previously rejected challenges to this patent family, all using **Sourcefire** as the primary reference
 - PAN challenged the '343 Patent (IPR2021-01155): **denied** institution
 - Cisco challenged related '193 Patent (IPR2018-01559): **denied** institution
 - Cisco challenged '193 Pat. again via ex parte re-exam: **claims re-issued**

POR at 6-9; Sur-Reply at 2-8

Emerging Threats (Ex. 1020)

- Text file of over 11,000 Snort rules
- Does not disclose or render obvious “applying... at least one packet transformation function configured to prevent an exfiltration operation” based on a determination that an application header field value matches second criterion specified by an operator
- Petitioner solely on relies on Rule 2003021
- Petitioner has shifted its theory to other Snort rules in its Reply in recognition of Rule 2003021’s flaws



It would not have been obvious to modify Sourcefire in view of Emerging Threats to yield the Claimed Rules “configured to prevent an exfiltration operation”
(Claims 1-20)

Undisputed Evidence For No Modification

- Many of Petitioner's Emerging Threats rules are commented-out and disabled (using “#” character)
- Undisputed extrinsic evidence shows a POSITA would understand Emerging Threat rules are commented out for having “excessive false positive” or “performance”

Commented rules can be for a number of reasons. @syoc is correct, the usual reasons are indeed for excessive false positives or the rule is just no longer relevant. Another common reason is poor performance. We (proofpoint/emerging threats) will include rules that we don't otherwise have coverage for but the rules don't perform well under QA. We include such rules, because we want to provide detection but don't want to enable it by default and cause sensors to potentially drop packets due to performance problems.

- Petitioner: could have vs. would have (“PO's declarants confirmed that commented-out rules could be enabled”)

Undisputed Evidence For No Modification

- All of Petitioner's Emerging Threats rules are “**alert**”, not “**drop**”
 - Petitioner asserts Sourcefire has the capability to set selectively rules to “alert” and “drop” (Pet. at 81, Ex. 1003 at ¶ 268-269)
 - **BUT:** This is not a trivial change
 - Undisputed direct and cross-examination testimony from former Emerging Threats employee showing a POSITA would know that “rules that are written to alert” would not have been flipped to drop traffic
 - *“these kind of rules were never designed to drop traffic... These rules exist to give evidence that some network administrator can correlated an event on the network with other events in order to start an investigation”*

POR at 12-13, 23-26; Sur-Reply at 4-8; Ex. 1101 at 54:5-14, 28:19-30:21;
Ex. 2031 at ¶ 6

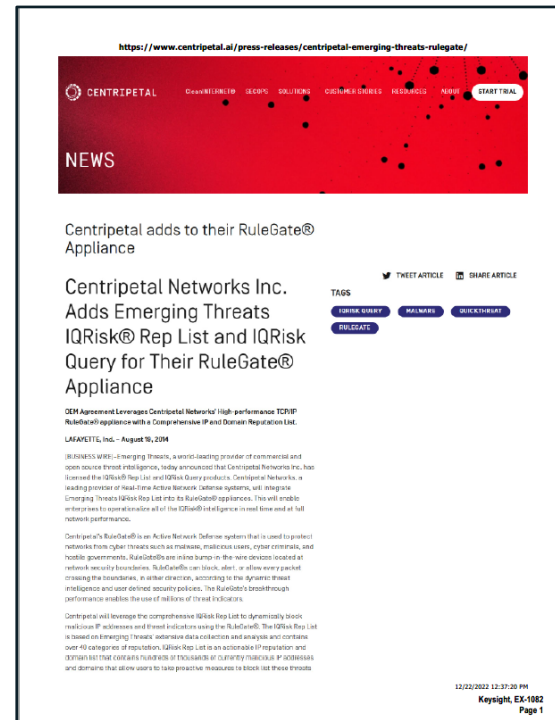
Undisputed Evidence For No Modification

- Petitioner's expert acknowledged the problem of false positives during on cross-examination:
 - “[I]f a product has a lot of false positives... it becomes unusable”
 - “[I]f you block too broadly, then obviously you block a user trying to get to an asset that's not in fact compromised”
- Petitioner's expert did not submit a Reply Declaration rebutting Mr. Marinho's testimony or reconciling his own cross-examination

POR at 12-13; Ex. 2010 at ¶ 68-70; Ex. 2011 at 33:6-21, 31:11-14

Hindsight Bias

- Petitioner relies on Centripetal press release (Ex. 1082) dated **August 19, 2014**, which post-dates the priority date of the '343 Patent as evidence of motivation to combine Sourcefire and Emerging Threats



POR at 23-26; Ex. 1082; Pet. at 37; Reply at 12-13; Ex. 1003 at ¶ 232-233

Emerging Threats: Rule 2003021

#Application data stream

#

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535
(msg:"ET POLICY TLS/SSL Encrypted Application Data on
Unusual Port SSLv3"; flowbits:isset,BS.SSL.Established;
flow:established,to_server; content:"|17 03 00|";
depth:4; threshold:typelimit, count 1, seconds 120,
track by_src; classtype:unusual-client-port-connection;
reference:url,doc.emergingthreats.net/2003021;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port;
sid:2003021; rev:8;)
```

Ex. 1020 at 109

Emerging Threats: Rule 2003021 (cont.)

- Cannot “prevent an exfiltration operation” because it is an **alert** rule
- Teaches nothing about exfiltration; Petitioner relies entirely on expert’s interpretation
- Rule’s msg + extrinsic evidence show the rule’s purpose was to flag certain SSL traffic on unusually high ports to “detect a new bot”
 - msg: “ET POLICY TLS/SSL Encrypted Application Data on Unusual Port SSLv3”
 - Ex. 2018, Ex. 2019, Ex. 2020: List-serv e-mails from Emerging Threats rule author describing his intention (“[t]he impetus to create [these rules] was a new bot that’s using standard ssl for a command and control session on a high port”)
- Petitioner’s “outdated version of SSL” theory is wrong and contrary to the evidence

POR at 14-19; Sur-Reply at 10-12; Ex. 2010 at ¶ 77-82;
Ex. 2018; Ex. 2019; Ex. 2020

Other Emerging Threat Rules

- Petitioner does not dispute other Rules **2002526**, **2002034**, **2001328** (cited elsewhere in Petition) do not render obvious the “prevent an exfiltration operation” claim limitation
- Petitioner’s Reply now argues Rules **2005319**, **2006409**, **2010234**, and **2003937**
 - But none of these apply the transformation function configured to prevent an exfiltration operation “**responsive to**” matching the application layer criteria

POR at 21-23; Sur-Reply at 12-14; Ex. 2010 at ¶ 77=82;
Ex. 2018; Ex. 2019; Ex. 2020

Untimely and Improper Use of Other ET Rules

- Petitioner cites to Rules **2005319**, **2006409**, **2010234**, and **2003937** in their Reply
 - Rules 2005319 and 2010234 only cited in original Petition for other dependent claims (improper incorporation of argument by reference)
 - Rules 2006409 and 2003937 are mentioned nowhere in the Original Petition

POR at 21-23; Sur-Reply at 12-14; Ex. 2010 at ¶ 77=82;
Ex. 2018; Ex. 2019; Ex. 2020

Emerging Threats: Rule 2005319

#from spyware LP data, by matt jonkman

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS  
(msg:"ET MALWARE Bizconcept.info Spyware Checkin";  
flow:to_server,established; content:"POST "; depth:5;  
nocase; uricontent:"/zuzu.php?&r="; nocase;  
classtype:trojan-activity;  
reference:url,doc.emergingthreats.net/bin/view/Main/2005319;  
reference:url,www.emergingthreats.net/cgibin/cvswb.cgi/sigs  
/MALWARE/MALWARE_Bizconcept.info; sid:2005319; rev:3;)
```

Ex. 1020 at 109

Emerging Threats: Rule 2006409

#idea from Blake Hartstein, use these only if you like. Not a definite indication of hostile activity

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET 81:65535
(msg: "ET POLICY HTTP POST on unusual Port Possibly Hostile";
flowbits:isnotset,BS.HTTP.ok; flow:established,to_server;
content:"POST"; nocase; depth:5; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2006409;
reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/POLICY/POLICY_HTTP_on_Off_Ports; sid:2006409;
rev:5;)
```

Ex. 1020 at 98

Emerging Threats: Rule 2010234

#by anon 4

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS
FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack HTTP Post 1";
flow:established,to_server; content:"POST"; depth:5;
uricontent:"/senm.php?data="; nocase; content:"data="; nocase; classtype:trojan-
activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName.TR
OJ_AGENT.GUZZ&VSect=T;
reference:url,www.threatexpert.com/report.aspx?md5=7ca709f154e6abc678fbc4df8a325
6b6; reference:url,www.threatexpert.com/threats/trojan-fraudpack-sd6.html;
reference:url,doc.emergingthreats.net/2010234;
reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010234; rev:4;)
```

Ex. 1020 at 18

Emerging Threats: Rule 2003937

by Joe Stewart

#

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN
Bandook iwebho/BBB-phish trojan leaking user data";
flow:established,to_server; content:"POST|20|/"; depth:6;
content:"|20|HTTP/1.1|0d0a|Content-Type|3a20|application/x-www-form-
urlencoded|0d0a|Host|3a20|"; within:150; content:"Content-
Length|3a20|"; within:100; content:"|0d0a0d0a|"; within:12;
content:"VISITED_URL"; within:100; classtype: trojan-activity;
reference:url,www.secureworks.com/research/threats/bbbphish;
reference:url,doc.emergingthreats.net/2003937;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003937; rev:4;)
```

Ex. 1020 at 155

Sourcefire in view of Emerging Threats Do Not Render Obvious “Allow[s], Based on a Determination That the Application Header Field Value Indicates a Request for Specified Resource Data, Each Packet of the Second Portion of Packets Indicating a Request for Specified Resource Data to Continue Toward its Respective Destination”
(Claims 5 and 12)

Evidence of Non-Obviousness / Secondary Considerations

Secondary Considerations

- Patent Office previously confirmed the objective indicia of nonobviousness supports the conclusion that Centripetal's exfiltration prevention tech is patentable (Ex. 1085 at 7)
- That same evidence is presented here again
 - Exs. 2023, 2024: Recognition of Problem, Long-Felt but Unresolved Need, Failure of Others
 - Exs. 2025, 2026, 2027, 2028: Industry Praise

POR at 27-34; Sur-Reply at 16-20

Emerging Threats (Ex. 1020) Does Not Qualify as Printed Publication

Emerging Threats is Not a Printed Publication

- “Publicly Accessible” vs. technically accessible
 - A reference is publicly accessible only if it was “disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.”
Acceleration Bay, LLC v. Avtivation Blizzard Inc., 908 F.3d 765 (Fed. Cir. 2018)
- Emerging Threats website (rules.emergingthreats.net) was not searchable or meaningfully indexed

There are the Emerging Threats.net Open rulesets.

More information available at <http://www.emergingthreatspro.com> and <http://www.emergingthreats.net>

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
blockrules/	10-Jan-2013 23:30	-	
changelogs/	11-Jan-2013 19:59	-	
fwrules/	11-Nov-2010 10:40	-	
open-nogpl/	25-Sep-2012 20:54	-	
open/	25-Sep-2012 20:54	-	
projects/	17-Jan-2011 12:34	-	
research/	05-Oct-2012 21:48	-	
version.txt	11-Jan-2013 19:59	5	